January 2021

SECURING CONNECTIVITY FAULT MANAGEMENT (CFM) CONTROL PACKETS USING STAMPED PASSPORT ATTESTATION

Karthik Babu Harichandra Babu

Eric Voit

Sujal Sheth

SECURING CONNECTIVITY FAULT MANAGEMENT (CFM) CONTROL PACKETS USING STAMPED PASSPORT ATTESTATION

AUTHORS:
Karthik Babu Harichandra Babu
Eric Voit
Sujal Sheth

ABSTRACT

Attestation is a trusted computing technology that can be applied to Ethernet layer operation, administration, and management (OAM) protocols, such as ethernet-cfm. A Canary Stamp is a collection of security evidence that demonstrates a sender's integrity and trustworthiness. Techniques presented herein provide for extending all types of Connectivity Fault Management (CFM) frames to carry a Canary Stamp Type-Length-Value object. Once a CFM frame is obtained by a receiver MEP, the receiver is to verify a sender's integrity and trustworthiness using the Canary Stamp TLV. CFM can add this trustworthiness status on each of its services in order to maintain connectivity between services and to verify the trustworthiness of maintenance endpoints (MEPs) and maintenance intermediate points (MIPs).

DETAILED DESCRIPTION

Ethernet Connectivity Fault Management (CFM), as defined in the Institute of Electrical and Electronics Engineers (IEEE) 802.1ag standard, includes various features, such as fault monitoring using the Continuity Check (CC) protocol (e.g., Continuity Check Message (CCM), etc.), oath discovery and fault verification using the link trace protocol (e.g., trace-routes), and fault isolation using the loopback protocol (e.g., Internet Protocol (IP) ping). CFM is commonly used at two levels: 1) by a service provider to check the connectivity among its provider edge (PE) routers, and 2) by a customer to check the connectivity among its customer edge (CE) routers.

A compromised device in a CFM domain can introduce various kind of denial-of-service (DOS) attacks, can learn device network topology, and/or can inject malicious CFM packets, such as false alarm indication signals, in order to trigger re-convergence of the network, which can introduce network traffic black holes. CFM is widely used in

different domains, such as IP networks, telecommunication networks, cloud networks, etc. to facilitate fault management for such networks. CFM is often deployed in IP / Multiprotocol Label Switching (MPLS) networks, Virtual extensible Local Area Networks (VxLANs), Virtual Private LAN Service (VPLS) networks, G8032 Ethernet Ring Protection System (ERPS) networks, etc. to verify end-to-end service connectivity.

To achieve secure packet transmissions involving the new packets for IEEE 802.1ag in a CFM network (e.g., CCM, Link Trace Message (LTM), Loop Back Message (LBM), Loop Back Reply (LBR), Link Trace Reply (LTR), etc. packets), it is important for destination devices to verify that CCM/LBM/LBR/LTM/LTR packets are only obtained from secure source devices.

When attestation of a peer node/device on a network (and proof that the peer node/device is not compromised) is desired, it is essential to first verify that the peer node/device has not been compromised before transmitting traffic to another peer node/device. Here, the Stamped Passport of Internet Engineering Task Force (IETF) "draft-voit-rats-trustworthy-path-routing" (as described in Section 3.6) can be used to verify that a link is being established to a trusted, uncompromised device. Following such verification, signaled changes to link bandwidth or other OAM messages can be trusted. For example, such verification could be applied to verify the trustworthiness of a Bandwidth Notification Message (BNM) received by router devices from third-party vendor radio devices in adaptive code modulation networks.

Techniques of this proposal extend support for validation of attested integrity data in order to establish trust between a source MEP and a destination MEP, including the MIPs in between their path. In particular, techniques herein can be used to apply attestation to protocols used in IEEE 802.1ag deployments.

Attestation is a trusted computing technology that can be applied to Ethernet layer OAM protocols, such as ethernet-cfm. A Canary Stamp is a collection of security evidence that demonstrates sender's Integrity and trustworthiness.

Consider an example CFM network, as shown below in Figure 1.

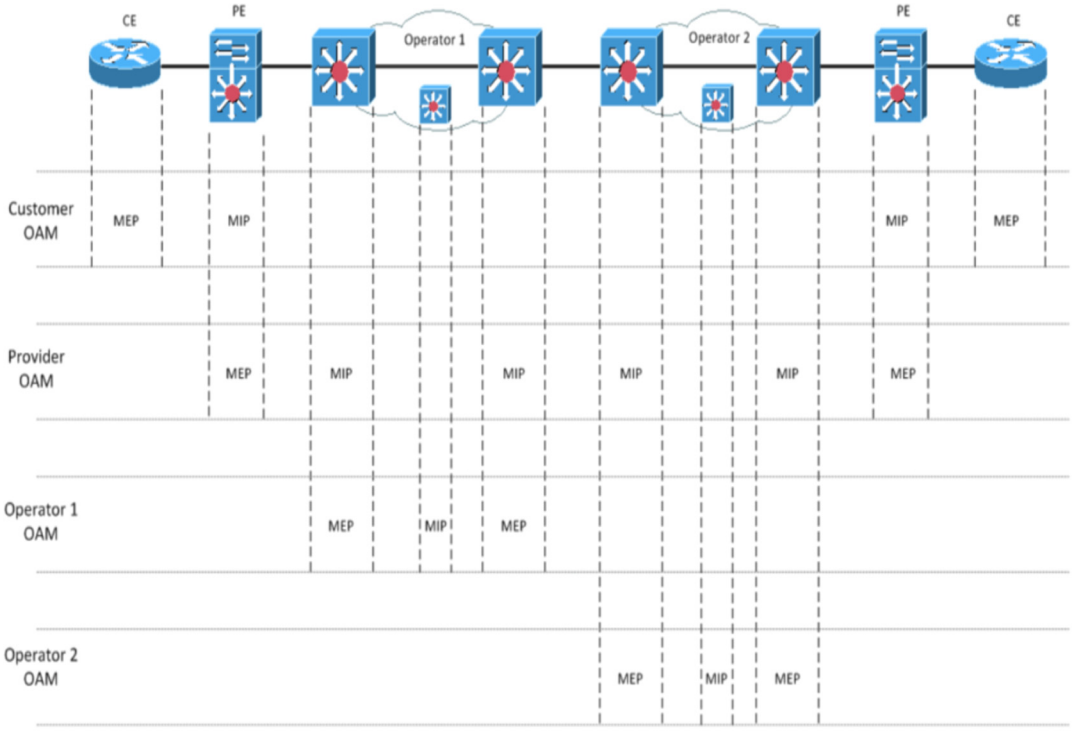

Figure 1: Example CFM network

Typically, CFM partitions the service network into various administrative domains. For example, operators, providers, and customers, as shown in Figure 1, might be part of different administrative domains. Each administrative domain is mapped into one maintenance domain and each maintenance domain is associated with a maintenance domain level from 0 through 7. Level allocation is based on the network hierarchy, where outermost domains are assigned a higher level than the innermost domains. Customer end points have the highest maintenance domain level.

In a CFM maintenance domain, each service instance is called a maintenance association. A maintenance association can be thought as a full mesh of maintenance endpoints (MEPs) having similar characteristics. MEPs are active CFM entities that generate and respond to CFM protocol messages.

CFM uses the Continuity Check (CC) protocol to announce its local port and interface status. CCM messages always use multicast destination Media Access Control (MAC) address and health check protocol that discovers and maintains adjacencies at the virtual LAN (VLAN) or link level (i.e., between MEPs). After a fault is detected, CFM can

utilize a loopback protocol or a link trace protocol to perform fault verification and isolation. The loopback protocol used in Ethernet OAM is modelled on the standard IP ping. The link trace protocol used in Ethernet OAM is modelled on the standard trace-route.

Techniques herein provided for extending all types of CFM frames to carry a Canary Stamp TLV object. Once obtained by a receiver MEP, the receiver MEP is to verify a sender's integrity and trustworthiness via the Canary Stamp TLV. CFM adds this trustworthiness status on each of its services running in order to maintain connectivity between the services and to verify the trustworthiness of MEP/MIP endpoints/intermediate points.

During operation, techniques herein involve adding a Stamped Passport into CFM CCM frames in which a CFM CCM sender periodically (e.g., based on a time interval, a number of frames sent, etc.) includes the new Canary Stamp TLV into the Stamped Passport. Each Canary Stamp TLV includes, at least in part, a current timestamp that is used to ensure the freshness of the Canary Stamp. Upon reception, a receiver verifies the information contained in the Canary Stamp. Support for a Stamped Passport can be added into the loopback protocol and the link trace protocol for CFM. Figure 2, below, illustrates example details associated with a Stamped Passport and Figure 3, below, illustrates example details associated with a CFM CCM frame that includes a number of Stamped Passports.

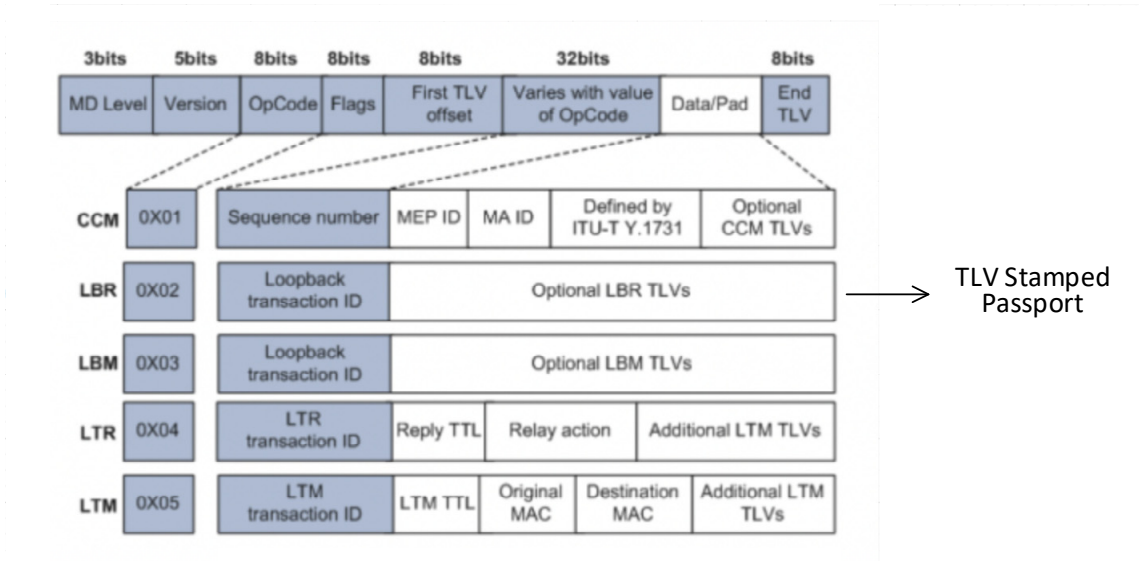

Figure 2: Stamped Passport Example Details

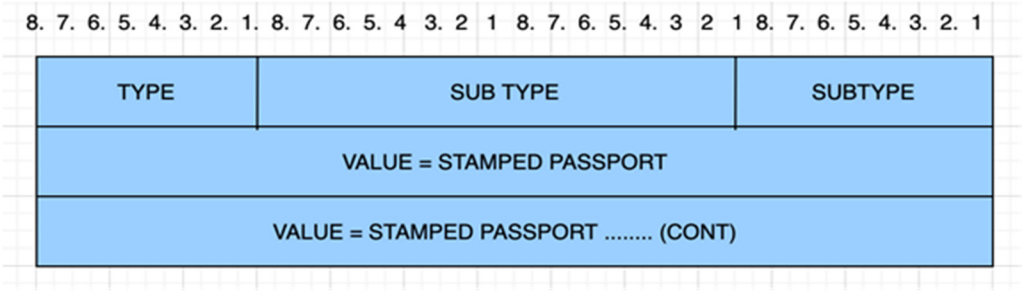

Figure 3: CFM CCM Frame Example Details

A new CCM/LBM/LBR/LTM/LTR Protocol Data Unit (PDU) type or a representation of the below data in packet is added to carry:

1. Metadata about the proof of integrity.
2. Proof of integrity. An example of this could include a signed "trustworthiness-vector" provided within the payload as defined by Section 3.6 of draft-voit-rats-trustworthy-path-routing (reference: https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/).
3. Proof of freshness of (2) by means of a signature over verifiably fresh data, such as the current time when the message is sent.

Accordingly, techniques herein can be used to attest the integrity of a source device and a destination device as well as provide link fault information for instances in which a fault may occur. Consider various example flows, as illustrated below in Figures 4 and 5.

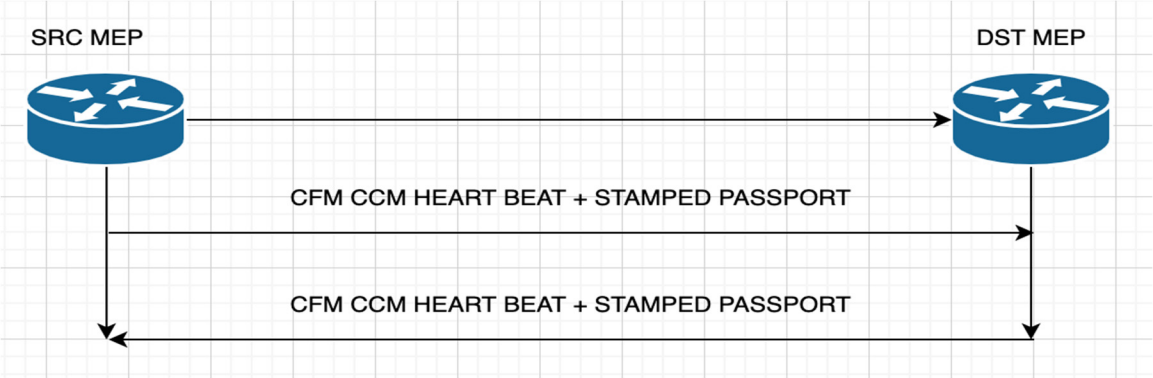

Figure 4: Example Flow Involving Source and Destination MEPs

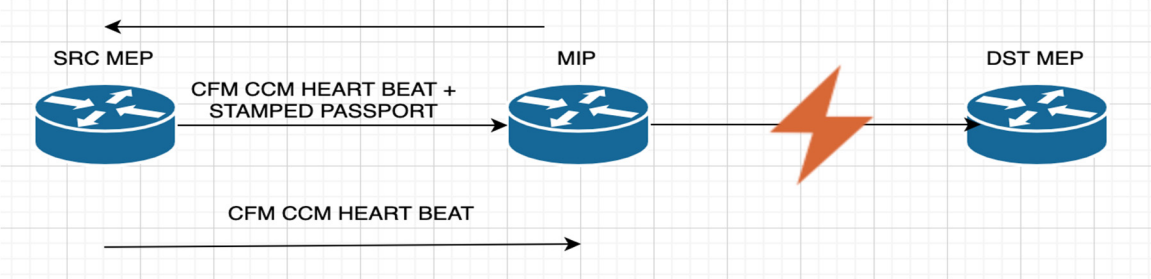

Figure 5: Example Flow involving a Source MEP and a MIP

During operation, when CFM message with attestation of integrity is received by an MEP device (as shown in Figure 4) or by a MIP device (as shown in Figure 5), the recipient device validates the integrity of the system from which the CCM/OAM packets were received. Based on the level of trust, various policies can be applied. For example, a policy may involve only selecting/connecting to a service on the device that offers a certain level of trust. For implementations in which such an attestation of integrity is included in a CFM CCM heart-beat, as shown in Figures 4 and 5, such a policy can be re-evaluated frequently. In another example, a policy can be granular based on the critical nature of a service that can be applied.

In summary, techniques herein provide for extending all types of CFM frames to carry a Canary Stamp TLV object that can be used by a receiver (MEP or MIP) to verify a sender's integrity and trustworthiness. This trustworthiness status can be provided for all CFM services in a CFM maintenance domain in order to maintain connectivity between the services and to verify the trustworthiness of MEP/MIP endpoints/intermediate points for the domain.